



# Service Delivery Program

## Case Study for Ashirvad Pipes

Prepared by Frontier Business Systems

## About the Customer:

Ashirvad Pipes is a leading manufacturer of uPVC and CPVC pipes, well-known for its innovative plumbing solutions in India. To maintain their industry leadership and continue providing top-quality products, they rely on a robust IT infrastructure. With growing operations, Ashirvad Pipes has adopted AWS Cloud to support their critical applications, including SAP workloads running on both Linux and Windows environments.

## Customer Challenge:

As Ashirvad Pipes expanded its cloud infrastructure, managing compliance, security, and governance across multiple AWS accounts became increasingly difficult. The company's primary challenges included:

1. **Manual Compliance Monitoring:** Ensuring compliance with internal security policies and external regulatory standards across a large number of AWS resources was time-consuming and prone to human error.
2. **Lack of Visibility:** There was limited visibility into configuration changes and security posture across AWS resources. This lack of insight made it difficult to enforce governance or detect unauthorized changes.
3. **S3 Data Security Concerns:** Ashirvad Pipes was concerned about the security of their sensitive data stored in Amazon S3. They wanted to ensure all S3 buckets were encrypted and secure, complying with best practices and industry standards.
4. **Cost of Managing Configuration Drift:** Identifying and remediating configuration drift across multiple accounts was both complex and costly.

## Partner Solution:

To address these challenges, Ashirvad Pipes partnered with Frontier Business Systems to implement a comprehensive solution based on **AWS Config**. The solution focused on compliance monitoring, S3 bucket security, and automation of remediation tasks.

Key components of the solution included:

1. **AWS Config for Continuous Compliance Monitoring:**
  - AWS Config was deployed across Ashirvad Pipes' AWS accounts to continuously track and record configuration changes in real-time.
  - Managed Config rules such as s3-bucket-server-side-encryption-enabled, cloud-trail-enabled, and iam-password-policy were implemented to ensure that the infrastructure followed security best practices.

- Custom Config rules were also developed to enforce specific internal policies.
- 2. **Automated Remediation Using AWS Systems Manager (SSM):**
  - AWS Config rules were integrated with **SSM Automation documents** to automatically remediate non-compliant resources. For example, if an S3 bucket was found to be unencrypted, an SSM automation document was triggered to apply server-side encryption.
- 3. **Centralized Visibility and Reporting:**
  - AWS Config provided a centralized view of Ashirvad Pipes' entire AWS infrastructure across multiple accounts.
  - The team set up **AWS Config Aggregators** to consolidate compliance reports from different AWS accounts into a single dashboard, making it easier to monitor and report on compliance.
- 4. **Amazon S3 Security:**
  - The solution included enforcing encryption for all Amazon S3 buckets using AWS Config rules and enabling logging through **AWS CloudTrail** for audit purposes.
  - AWS Config snapshot and history files were utilized for security analysis, providing a clear record of historical configuration changes.

## **Results and Benefits:**

1. **Enhanced Compliance and Security:**
  - Ashirvad Pipes gained real-time visibility into the compliance state of their AWS resources, ensuring adherence to both internal and external security policies.
  - The automation of configuration checks and remediation significantly reduced the risk of non-compliance and configuration drift.
  - All Amazon S3 buckets are now encrypted, providing peace of mind for data security.
2. **Improved Operational Efficiency:**
  - By automating compliance checks and remediation tasks, the IT team at Ashirvad Pipes was able to focus on higher-value activities rather than manual configuration management.
  - Centralized visibility through AWS Config aggregators streamlined monitoring, reducing the time and effort required to maintain compliance across multiple AWS accounts.
3. **Cost Savings:**
  - The implementation of automated compliance checks and remediation reduced the costs associated with manual monitoring and troubleshooting of configuration issues.
  - By proactively managing compliance and security, Ashirvad Pipes was able to avoid potential penalties and data breaches, which could have incurred significant financial and reputational costs.

#### **4. Future-Proofing:**

- The solution laid a foundation for scalable governance as Ashirvad Pipes continues to grow its cloud infrastructure. With AWS Config in place, they are well-positioned to adapt to future security and compliance requirements.

#### **About the Partner**

Frontier Business Systems Private Limited, headquartered in Bengaluru, Karnataka, is a leading IT service provider specializing in virtualization consulting, IT infrastructure management, and information security solutions. With extensive experience in cloud computing, Frontier offers a wide range of services tailored to help businesses enhance their infrastructure while ensuring operational continuity. Frontier holds several AWS Competencies, which validate their technical expertise and proven success in delivering AWS solutions. Their specialization in cloud migration, security, and managed services helps clients, like Ashirvad Pipes, achieve their goals through scalable, secure, and efficient cloud solutions.